Supplement for MAA 3200, Prof S Hudson, Fall 2018
Constructing Number Systems

A major goal of this course is to construct the number systems N, Z and Q, and especially the real numbers R, which play such a central role in mathematics. We need to understand the properties these systems have in common and also how they differ. Why is the real number system the standard choice in courses like Calculus? We can only spend about a week on this, but it will be good practice with proof-writing, equivalence relations, partial orders, functions, and an introduction to Algebra in general.[1]

Every basic term, such '0', '+' and '<' can be defined precisely.[2] Every well-known fact and formula, such as $n + m = m + n$, can be proven. I will provide some sample proofs, as time permits, and welcome any questions about the rest. These web page notes should be enough to outline the main definitions and sample theorems. You can also find this material in the optional text by Morash, in much more detail. I can put it on reserve in our library upon request.

I. Outline of the Construction

A) The natural numbers, N.

1) Define N as a set.
2) Define $+$ on N and prove formulas [like $n + m = m + n$, etc].
3) Define nm on N and prove related formulas.
4) Define $<$ on N and prove prove related formulas.

B) The integers, Z, with 4 steps similar to those done in A). We'll also introduce subtraction, absolute value, etc.

C) The rational numbers, Q, with steps as in B), plus division, etc.

D) The real numbers, R, with the steps in C), plus completeness, etc.[3]

The main methods in part A) are recursive definitions and inductive proofs. In B) we define Z as equivalence classes in NxN. The rest of

[1] here, Algebra refers to a somewhat advanced study of structures like groups, fields, vector spaces, etc.

[2] a possible exception is that we must accept the existence N, at least as a set.

[3] This involves some basic topology and analysis. I plan to defer most of this until we have covered Cauchy sequences, maybe in the last weeks of the term. Read over the main properties of R in Kane, Ch. 2.5, or perhaps in Morash.

B) goes quickly and is based heavily on A). Likewise, C) builds on B) and D) builds on C). Completing all these steps would take months, so we will cover A), B) and C) rather lightly now and focus more on D) later.

II. Some details of Part A); Constructing N

We want to define N and its binary operations $+$ and $\cdot$ and to prove some of their properties.[4] A *binary operation* on a set A is a function $f : A \times A \to A$. For example, we are planning to define a binary operation $f(n, m) = n + m$.

In the following axiom (a primitive definition of N), the notation $\sigma(m)$ refers to the next number after m. So, $\sigma(17) = 18$, for example. Later on, we can say $\sigma(m) = m + 1$, but "+" hasn't been defined yet.[5]

Axiom: There is a set N and a mapping $\sigma : N \to N$ such that:
a) σ is 1-1, but not onto; there's an element $0 \in N$ not in rng (σ). And
b) If $S \subseteq N$ and $0 \in S$ and $\forall m \in N$, $(m \in S \to \sigma(m) \in S)$ then $S = N$.[6]

The induction method is based on part b), and is the main tool in proofs about N. The next steps aim to define "+", using a function $s_m(n)$ (which, in effect, adds m to n). For each m, this function is defined recursively on $n \in N$.

Thm: $\forall m \in N$ there is a unique function $s_m : N \to N$ such that
a) $s_m(0) = m$ and
b) $\forall n \in N$, $s_m(\sigma(n) = \sigma(s_m(n))$.[7]

Def: Given any $m, n \in N$ their *sum* is $s(m, n) = s_m(n)$; it may also be written "$m + n$".

[4] You may enjoy this more by pretending that you have not seen these things before!

[5] and neither has '1'. We will define 1, but will not bother to define many specific numbers like 17, etc.

[6] Notice that this uses the convention that $0 \in N$. In textbooks that do not use include 0, the whole presentation of N will vary a bit. However, this is ultimately a minor issue, which I will ask you to deal with, if you read those books.

[7] In my 2013 file, Part a) was $s_m(1) = \sigma(m)$. Probably I was following some book that did not include 0 in N. In this 2018 version, we can set $n = 0$ in Part b, and infer that $s_m(1) = \sigma(m)$ (where 1 is defined to be $\sigma(0)$).

Part b says $m+(n+1) = (m+n)+1$ but without using '+' I plan to prove a few theorems like this one in class, but not in this file. See Morash, etc, if interested in more proofs.

Thm: N is closed under addition, and $m+n = n+m$. [We will state and prove a few theorems like this, but won't have time for too many]. The next steps aim to define multiplication recursively on N.

Def: For each $m \in N$ let $p_m : N \to N$ be such that a) $p_m(0) = 0$, and b) $\forall n \in N$, $p_m(\sigma(n)) = p_m(n) + m$. Define the product (often written $m \cdot n$ or just mn) by $p(m,n) = p_m(n)$.

Sample theorems: $mn = nm$ and $m(n+k) = mn + mk$.

Def: $a < b$ means $\exists c \neq 0$ in N such that $a + c = b$.

Thm: If $a < b$ then $a \neq b$; and $\forall c \in N,\ a + c < b + c$; and $<$ has the transitive property.

Thm (trichotomy) Given any $a, b \in N$ exactly one of these three is true: $a < b$, $b < a$ or $a = b$.

For practice, try proving some of these theorems. I plan to assign some of this as HW on a separate page. At this point, you may not be able to prove everything above, but you should understand N well enough to move on to Z. You should also be getting a feel for what has to be done in constructing new systems. If you have any questions at all about N, now is the time ! We can pause for more proofs here if people are interested.

III. About Z and Q

Our first goal is to define Z as a set.[8] With N as a tool, this section is actually easier than the previous one.

Def: Let $A = N \times N$. Define a relation $\sim$ on A by: $(a,b) \sim (c,d)$ means $a + d = b + c$.

Thm: This is an equivalence relation on A.[9]

Def: Let $Z = A/\sim$ be the set of equivalence classes, and call the elements of Z *integers*.

[8] You might expect definitions of $-1, -2, \ldots$ at this point, but the method below is a little cleaner.

[9] This was a TF question on Exam I, and is not very hard to prove.

You can think of $[(a, b)]$ as the integer $a - b$. For example, (3,5) and (10,12) are in the same eq. class, and they both correspond to the element $-2 \in Z$.[10]

Now, we'll define $+$ and $\cdot$ on Z.

Def: The *sum* of two integers is $[(a, b)] + [(c, d)] = [(a + c, b + d)]$.
Def: The *product* of two integers is $[(a, b)] \cdot [(c, d)] = [(ac+bd, bc+ad)]$.

For example, [(3,5)]+[(7,2)] = [(10,7)], which corresponds to the more familiar -2+ 5 = 3. Notice that [(3,5)]=[(10,12)]. If we use (10,12) instead of (3,5), to do the sum, do we still get the same answer? Yes, we get [(17, 14)], which is the same as [(10,7)]. If this could fail, then the definition above is bad. The next theorem says sums always work out well, also multiplications.

Thm: These two operations are *well-defined*.

Thm: There is a unique integer $a \in Z$ such that $\forall x \in Z, a + x = x + a = x$. We call this integer "0".

Thm: For each $z \in Z$, there is a unique $y \in Z$ such that $z + y = y + z = 0$. We write "$y = -z$" and call this the additive inverse of z.[11]

Number systems with nice properties like the ones above get special labels like *groups, rings and fields.* Z is not a field because it doesn't have multiplicative inverses, but our theorems do imply that Z is a *ring.* N is not even a ring, since it doesn't have additive inverses. You may learn more properties of groups, rings and fields in an *Algebraic Structures* course. Next, we define $<$ on Z using the relation $<$ defined on N:

Def: Let $x = [(a, b)]$ and $y = [(c, d)]$. Then $x < y$ means $a + d < b + c$.[12].

[10] This version of Z is 'not exactly the usual Z', but the two versions have the same structure. So, we say that the two versions are *isomorphic*, and treat them as the same. We can talk about this more if you like - otherwise I will treat this as a mere technicality and go on. Similar comments apply to the Q and R that we will define soon.

To keep this file short, I did not include a separate theorem that $N \subset Z$. It might be more accurate (but pretty unusual) to say that 'the Z defined here contains a subset isomorphic to N'. Again, this is a technicality.

[11] We can define substraction now, by $x - z = x + (-z)$. But this is easy and it usually gets less attention than addition.

[12] (a) The formula $a + d < b + c$ is in N, hence already defined. (b) We should ask whether $<$ is well-defined, as we did for $+$. The answer is Yes, and there is a

There are many more simple theorems about Z. Example: if $x < y$ and $0 < z$, then $xz < yz$. We'll look at some of these in class or in HW exercises. Define $>$ as the inverse relation of $<$. Define $\leq$ as the relation $= \cup <$.

Lets move on and define Q,[13] using Z. It is similar to what we just did, constructing Z from N. Let $A = Z \times Z^+$ and define $\sim$ on A by: $(p, q) \sim (r, s)$ means $ps = rq$. Let $Q = A/$.

Ex: $(2, 3) \sim (4, 6)$ and both ordered pairs may be thought of as $2/3$. We can now define $+$, $\cdot$ and $<$ on Q using Z. The definition below is based on the familiar formulas $\frac{p}{q} + \frac{r}{s} = \frac{ps+rq}{qs}$ and $\frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs}$.

Def: Let $x = [(p, q)]$ and $y = [(r, s)]$. Then set $x + y = [(ps + rq, qs)]$ and $xy = [(pr, qs)]$.

Thm: Q is a *field*, which means the operations defined above satisfy the field axioms.[14].

An *ordered* field is one with a relation $<$ defined on it, that satisfies the order axioms. Define $x < y$ to mean $y - x \in P = \{[(p, q)] \in Q \mid pq > 0\}$, which is the set of *positive* rational numbers. Theorem (not proved here): With this definition, Q is an ordered field.

All this makes Q pretty useful, but it is not the most useful field, because it is not *complete* (see Kane Ch. 2.5.2 or the definition below). Later, we'll discuss why that is a problem, for doing calculus, for example. We will eventually resolve this, by defining the better system R, which is the only complete ordered field. The complex numbers C form another complete field, also very useful, but it is not an ordered field.[15]

Quite a few theorems can be proven directly from the field axioms, which means we don't have to prove them all separately for Q and R and C. Let F stand for any field.

Sample Thm: For all $x \in F$, $x \cdot 0 = 0$.

theorem for that, but to keep this file short, I will usually treat *well-defined* as a technicality, and not mention it every time. (c) For brevity, I omit the definition of $|x|$ in Z and Q. It is rather important, but easy.

[13] we will also define + etc on Q. Since all this is much more than one simple definition, the process is usually called *constructing* Q.

[14] Roughly, in a field you can *divide*, and this has some nice familiar properties. You can read about fields, and ordered fields in many places, such as Kane Ch.2.5

[15] the interpretation of *complete* is a bit different for C, since it is not ordered. We will not pursue this.

Sample Thm: If F is ordered then $1 > 0$, and if $x > 0$ then $x^{-1} > 0$. Also, we can define $\leq$ and $|x|$ the usual way, and then $\leq$ is a partial order on F.

Def: An ordered field F is *complete* if every nonempty set S with an upper bound has a least upper bound - also known as a *supremum.* (See Velleman page 197 or Kane page 35. Lower bounds could be used instead; they are similar).

Ex: Let $F = Q$ and let $S = \{x \in Q |\ x^2 < 2\}$. If F were R the lub would be $\sqrt{2}$, but since that doesn't belong to $F = Q$, S has no lub (proof omitted). So, Q is not complete. It has "holes" at places like $\sqrt{2}$. Many theorems, such as the Intermediate Value Theorem, would fail if this field were used in Calculus instead of R.

Next: We will postpone the construction of R because I consider Chs 3 and 4 of Kane's book more important, and because we will need the concept of a Cauchy sequence from Ch. 3.5.7. Using R to learn Cauchy, and Cauchy to construct R may seem circular. But the Cauchy concept also makes sense when $F = Q$, so our presentation will not actually be circular.

To go on, you should know Ch.2.5 of Kane pretty well - and just accept for now that it is all true. You do not need to memorize perfectly the field axioms, but should have good idea of them. For Exam 2, you should do the HW for this file (from a separate file). You don't need to know proofs of every theorem here, but probably should be able to handle some of the easier ones, or maybe the ones done in class. Know the basic ideas, definitions and notations in this file.

Summary: Numbers in Z and Q [and later on, R too] are equivalence classes formed from earlier number systems. Binary operations such as '+' are functions. Those, and relations such as '<' are defined in natural ways using previous number systems (and you should know these definitions). For the first system, N, recursion and induction are needed. Get comfortable enough with σ, s_m and p_m to write simple proofs about N, mostly using induction. Understand the issue of 'well-defined', and at least roughly, 'isomorphism'.